

## \* NOTICES \*

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

CLAIMS

---

## [Claim(s)]

[Claim 1] The terminal which can detect the identification information of a pocket transmitter to the pocket transmitter concerned which prepares for the location which is going to receive authentication and an individual owns, It is a personal authentication system containing management equipment equipped with a storage means by which the identification information and the password code of a pocket transmitter required in order to connect with this terminal through a communication line and to attest an individual were memorized by relating. The above-mentioned terminal is what detects the identification information of a pocket transmitter, turns this detected identification information to the above-mentioned management equipment, and transmits. The above-mentioned management equipment It checks whether when identification information and a password code are received from a pocket transmitter, this received password code is in agreement with the password code which relates with the identification information of the pocket transmitter concerned, and is memorized by the above-mentioned storage means. When it memorizes that there was an application of authentication from the individual who owns the pocket transmitter concerned when in agreement, and identification information is received from the above-mentioned terminal after that The personal authentication system characterized by being what transmits the answer of Authentication O.K. towards the above-mentioned terminal when it checks whether there had been any application of authentication before from the pocket transmitter specified by this identification information that received and it is checked that there had been an application of authentication.

[Claim 2] It is the personal-authentication system according to claim 1 carry out containing a means transmit the completion signal of password code reception to the pocket transmitter concerned when it is memorized that the above-mentioned management equipment had the application of authentication from the individual who owns the pocket transmitter concerned in accordance with the password code with which the password code received from the pocket transmitter relates with the identification information of the pocket transmitter concerned, and is remembered to be by the above-mentioned storage means as the description.

[Claim 3] The terminal which can detect the identification information of a pocket transmitter to the pocket transmitter concerned which prepares for the location which is going to receive authentication and an individual owns, It is a personal authentication system containing management equipment equipped with a storage means by which the identification information and the password code of a pocket transmitter required in order to connect with this terminal through a communication line and to attest an individual were memorized by relating. The above-mentioned terminal is what detects the identification information of a pocket transmitter, turns this detected identification information to the above-mentioned management equipment, and transmits. The above-mentioned management equipment When the identification information of a pocket transmitter was received from the above-mentioned terminal and the password code which calls the pocket transmitter specified by this identification information, answers this call after that, and is automatically transmitted from a pocket transmitter is received Check whether this received password code is in agreement with the password code which relates with the identification information of the pocket transmitter concerned, and is memorized by the above-mentioned storage means, and when it is checked that it is in agreement The personal authentication system characterized by being what transmits the answer of Authentication O.K. towards the above-mentioned terminal.

[Claim 4] It is the approach of attesting the individual using the pocket transmitter which an individual owns. With a pocket transmitter The identification information and the password code of the pocket transmitter concerned are beforehand transmitted to management equipment. The terminal which the terminal with which the location which is going to receive authentication was equipped was made to detect the identification information of a pocket transmitter, and detected the identification information of this pocket transmitter A communication line is minded for the detected identification information. To the above-mentioned management equipment delivery and the above-mentioned management equipment It checks whether when identification information and a password code are received from a pocket transmitter, this received password code is in agreement with the password code which relates with the identification information of the pocket transmitter concerned, and is memorized by the storage means. When it memorizes that there was an application of authentication from the individual who owns the pocket transmitter concerned when in agreement, and identification information is received from the above-mentioned terminal after that The personal authentication approach characterized by transmitting the answer of Authentication O.K. towards the above-mentioned terminal when it checks whether there had been any application of authentication before from the pocket transmitter specified by this identification information that received and it is checked that there had been an application of authentication.

[Claim 5] It is the approach of attesting the individual using the pocket transmitter which an individual owns. Input a password code beforehand, store it in a pocket transmitter, and the terminal with which the location which is going to

receive authentication was equipped is made to detect the identification information of a pocket transmitter. The terminal which detected the identification information of this pocket transmitter A communication line is minded for the detected identification information. To management equipment delivery and management equipment If the identification information of a pocket transmitter is received from the above-mentioned terminal, the pocket transmitter specified by this identification information will be called. This call a carrier beam pocket transmitter The management equipment which turned to management equipment automatically the password code which it was beforehand inputted and has been memorized, transmitted, and received the password code from the pocket transmitter The personal authentication approach which checks whether this received password code is in agreement with the password code which relates with the identification information of the pocket transmitter concerned, and is memorized by the storage means, and is characterized by transmitting the answer of Authentication O.K. towards the above-mentioned terminal when it is checked that it is in agreement.

[Claim 6] It is management equipment for personal authentication systems which attests the individual using the pocket transmitter which an individual owns. While the terminal installed in the location which is equipped with a storage means by which the identification information and the password code of a pocket transmitter required in order to attest an individual were memorized by relating, and is going to receive authentication is connected When a pocket transmitter and a communication link are possible and identification information and a password code are received from a pocket transmitter It checks whether this received password code is in agreement with the password code which relates with the identification information of the pocket transmitter concerned, and is memorized by the above-mentioned storage means. When it memorizes that there was an application of authentication from the individual who owns the pocket transmitter concerned when in agreement, and identification information is received from the above-mentioned terminal after that Management equipment characterized by being what transmits the answer of Authentication O.K. towards the above-mentioned terminal when it checks whether there had been any application of authentication before from the pocket transmitter specified by this identification information that received and it is checked that there had been an application of authentication.

---

[Translation done.]

\* NOTICES \*

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the management equipment for a personal authentication system, the personal authentication approach, and personal authentication systems which attests an individual using a pocket transmitter.

[0002]

[Description of the Prior Art] For example, when paying a goods price with a credit card, or in case the cash dispenser (CD) machine installed in the bank etc. draws out cash, authentication (personal authentication) of the user of a credit card or a cash dispenser is performed. Although it is common to be carried out based on the information currently recorded on the credit card or the ATM card as for this personal authentication, recently, the technique of performing personal authentication using portable telephones, such as a system currently indicated by JP,11-45366,A, for example, is proposed.

[0003] In the system currently indicated by the above-mentioned open official report, in case a shopper pays the price of the goods purchased at the store, he connects his own portable telephone to the terminal currently installed in the store. If a portable telephone and a terminal are connected, reading appearance of the call number (cellular-phone number) of a portable telephone will be carried out to a terminal, and the call number by which reading appearance was carried out will be transmitted to the computer which is carrying out generalization management of the system. Then, based on the call number sent to the computer, a shopper's portable telephone is called from a computer. If it shows around so that a password code may be inputted from a computer, if a shopper answers this call, and a shopper inputs a password code into a portable telephone according to this advice, that password code will be transmitted to a computer. If the call number of a portable telephone and the password code given to that owner are beforehand associated and registered into the computer and a password code is sent from a portable telephone, this sent password code and the password code registered will be attested with those who inputted the password code into that portable telephone being owners of a portable telephone, if collating is performed and these password codes are in agreement. In this way, if authentication is made, a goods price will be charged directly to the bank account of the owner of a portable telephone later.

[0004]

[Problem(s) to be Solved by the Invention] As mentioned above, in the system currently indicated by the above-mentioned open official report, if it answers that waiting and a portable telephone were called and a password code is inputted after connecting a portable telephone to a terminal until a portable telephone is called from a computer, the inputted password code will be transmitted to a computer, and authentication will be performed. Therefore, after connecting a portable telephone to a terminal before authentication is completed, long time amount starting and a shopper may be irritated. Moreover, when especially the store is crowded and authentication takes time amount, other shoppers will be kept waiting and even other shoppers and salesclerks of these may make it irritated.

[0005] Then, the object of this invention is offering the management equipment for a personal authentication system, the personal authentication approach, and personal authentication systems which can shorten the time amount which solves an above-mentioned technical technical problem and authentication takes.

[0006]

[The means for solving a technical problem and an effect of the invention] Invention according to claim 1 for attaining the above-mentioned object The terminal which can detect the identification information of a pocket transmitter to the pocket transmitter concerned which prepares for the location which is going to receive authentication and an individual owns. It is a personal authentication system containing management equipment equipped with a storage means by which the identification information and the password code of a pocket transmitter required in order to connect with this terminal through a communication line and to attest an individual were memorized by relating. The above-mentioned terminal is what detects the identification information of a pocket transmitter, turns this detected identification information to the above-mentioned management equipment, and transmits. The above-mentioned management equipment It checks whether when identification information and a password code are received from a pocket transmitter, this received password code is in agreement with the password code which relates with the identification information of the pocket transmitter concerned, and is memorized by the above-mentioned storage means. When it memorizes that there was an application of authentication from the individual who owns the pocket transmitter concerned when in agreement, and identification information is received from the above-mentioned terminal after that When it checks whether there had been any application of authentication before from the pocket transmitter specified by this identification information that received and it is checked that there had been an application of authentication, it is the personal authentication system characterized by being what transmits the

answer of Authentication O.K. towards the above-mentioned terminal.

[0007] According to this invention, since a password code is transmitted to management equipment from a pocket transmitter and it is checked for the password code at this time whether it is the right, when management equipment receives the identification information of a pocket transmitter from a terminal, it is not necessary to check response relation between this identification information and a password code. Therefore, the pocket transmitter with which management equipment is identified by the identification information (cellular-phone number etc.) of a pocket transmitter which received from the terminal can be called, and the time amount taken [ after there is this call and a transmitter identification information receiving means receives transmitter identification information compared with the conventional technique which inputs a password code and is transmitted to management equipment ] to complete personal authentication can be shortened.

[0008] In addition, when it is memorized that there was an application of authentication from the individual to whom the password code according to claim 2 which received the above-mentioned management equipment from the pocket transmitter like owns the pocket transmitter concerned in accordance with the password code which relates with the identification information of the pocket transmitter concerned, and is memorized by the above-mentioned storage means, it is desirable in containing a means transmit the completion signal of password code reception to the pocket transmitter concerned. In this case, since the completion signal of password code reception is transmitted to a pocket transmitter, the individual who transmitted the password code to management equipment from the pocket transmitter can know whether the transmitted password code was a right thing.

[0009] The terminal which can detect the identification information of a pocket transmitter to the pocket transmitter concerned which the location which is going to receive authentication is equipped with invention according to claim 3, and an individual owns, It is a personal authentication system containing management equipment equipped with a storage means by which the identification information and the password code of a pocket transmitter required in order to connect with this terminal through a communication line and to attest an individual were memorized by relating. The above-mentioned terminal is what detects the identification information of a pocket transmitter, turns this detected identification information to the above-mentioned management equipment, and transmits. The above-mentioned management equipment When the identification information of a pocket transmitter was received from the above-mentioned terminal and the password code which calls the pocket transmitter specified by this identification information, answers this call after that, and is automatically transmitted from a pocket transmitter is received Check whether this received password code is in agreement with the password code which relates with the identification information of the pocket transmitter concerned, and is memorized by the above-mentioned storage means, and when it is checked that it is in agreement It is the personal authentication system characterized by being what transmits the answer of Authentication O.K. towards the above-mentioned terminal.

[0010] If according to this invention the password code is inputted into the pocket transmitter in advance of transmission of the transmitter identification information to management equipment and the call of the pocket transmitter from management equipment is answered, that password code inputted by preceding will be automatically transmitted towards management equipment. Thereby, after there is a call of a pocket transmitter from management equipment, a password code can be inputted into a pocket transmitter and the time amount which personal authentication takes can be shortened compared with the conventional technique which turns this inputted password code to management equipment, and is transmitted.

[0011] Invention according to claim 4 is the approach of attesting the individual using the pocket transmitter which an individual owns. With a pocket transmitter The identification information and the password code of the pocket transmitter concerned are beforehand transmitted to management equipment. The terminal which the terminal with which the location which is going to receive authentication was equipped was made to detect the identification information of a pocket transmitter, and detected the identification information of this pocket transmitter A communication line is minded for the detected identification information. To the above-mentioned management equipment delivery and the above-mentioned management equipment It checks whether when identification information and a password code are received from a pocket transmitter, this received password code is in agreement with the password code which relates with the identification information of the pocket transmitter concerned, and is memorized by the storage means. When it memorizes that there was an application of authentication from the individual who owns the pocket transmitter concerned when in agreement, and identification information is received from the above-mentioned terminal after that When it checks whether there had been any application of authentication before from the pocket transmitter specified by this identification information that received and it is checked that there had been an application of authentication, it is the personal authentication approach characterized by transmitting the answer of Authentication O.K. towards the above-mentioned terminal.

[0012] According to this approach, the effectiveness described in relation to claim 1 and the same effectiveness can be acquired. Invention according to claim 5 is the approach of attesting the individual using the pocket transmitter which an individual owns. Input a password code beforehand, store it in a pocket transmitter, and the terminal with which the location which is going to receive authentication was equipped is made to detect the identification information of a pocket transmitter. The terminal which detected the identification information of this pocket transmitter A communication line is minded for the detected identification information. To management equipment delivery and management equipment If the identification information of a pocket transmitter is received from the above-mentioned terminal, the pocket transmitter specified by this identification information will be called. This call a carrier beam pocket transmitter The management equipment which turned to management equipment automatically the password code which it was beforehand inputted and has been memorized, transmitted, and received the password code from the pocket transmitter It checks whether this received password code is in agreement with the password code which relates with the identification information of the pocket transmitter concerned, and is memorized by the storage means, and when it is checked that it is in agreement, it is the personal authentication approach characterized

by transmitting the answer of Authentication O.K. towards the above-mentioned terminal.

[0013] According to this approach, the effectiveness described in relation to claim 3 and the same effectiveness can be acquired. Invention according to claim 6 is management equipment for personal authentication systems which attests the individual using the pocket transmitter which an individual owns. While the terminal installed in the location which is equipped with a storage means by which the identification information and the password code of a pocket transmitter required in order to attest an individual were memorized by relating, and is going to receive authentication is connected. When a pocket transmitter and a communication link are possible and identification information and a password code are received from a pocket transmitter. It checks whether this received password code is in agreement with the password code which relates with the identification information of the pocket transmitter concerned, and is memorized by the above-mentioned storage means. When it memorizes that there was an application of authentication from the individual who owns the pocket transmitter concerned when in agreement, and identification information is received from the above-mentioned terminal after that. When it checks whether there had been any application of authentication before from the pocket transmitter specified by this identification information that received and it is checked that there had been an application of authentication, it is management equipment characterized by being what transmits the answer of Authentication O.K. towards the above-mentioned terminal.

[0014] In the personal authentication system using the management equipment of this invention, the effectiveness described in relation to claim 1 and the same effectiveness can be acquired.

[0015]

[Embodiment of the Invention] Below, the gestalt of implementation of this invention is explained to a detail with reference to an accompanying drawing. Drawing 1 is the block diagram showing the whole personal authentication system configuration concerning 1 operation gestalt of this invention. It is the system used when the shopper who did some shopping at the store in a town etc. pays a goods price by credit payment (how to pay a goods price, without paying cash at a store when a goods price is charged directly to a bank account by later), and the portable telephone 1 which each shopper owns is used for this personal authentication system. The memory which is not illustrated is built in the portable telephone 1, and the call number (cellular-phone number) and the owner for calling a portable telephone 1 can make this memory memorize the number which operated and inputted the input key 11 now.

[0016] The store terminal 2 for performing personal authentication is installed in each store. The store terminal 2 is connected to the management equipment 3 installed in the credit firm which does generalization management of this personal authentication system, the bank, etc. (henceforth a "systems operation firm") through the communication line. Moreover, management equipment 3 can perform data communication now between portable telephones 1 through a telephone network. Management equipment 3 is equipped with the storage 31 for memorizing the file according to individual. The file according to individual is created when an individual contracts the utilization agreement of a personal authentication system with a systems operation firm, it is memorized by storage 31, and includes information, such as a bank account of the individual for charging directly the password code and goods price which were given to the cellular-phone number of the individual (shopper) portable telephone 1, and the individual. An individual can determine a password code in the case of the utilization agreement of for example, a personal authentication system, and it consists of combination of two or more figures or an alphabetic character. That is, information, such as a cellular-phone number required for personal authentication, a password code, and a bank account, is mutually related with the storage 31 of management equipment 3, and it memorizes according to the individual.

[0017] For example, in advance of payment of the goods price, the shopper who is going to pay a goods price by credit payment calls management equipment 3 from his own portable telephone 1, operates the input key 11 of a portable telephone 1, and transmits a password code to management equipment 3. The memory of a portable telephone 1 may be made to memorize the call number of management equipment 3 beforehand, whenever it calls management equipment 3, it may operate an input key 11, and it may input. Moreover, the memory built in the portable telephone 1 may be made to memorize beforehand, whenever it calls management equipment 3, an input key 11 may be operated, and a password code may also input. However, when the case where the theft of the portable telephone 1 is carried out, and a portable telephone 1 are lost, in order to prevent that reading appearance of the password code is carried out, and it is used improperly from the memory of a portable telephone 1, after predetermined time (for example, for 2 minutes) passes since the writing, it is desirable [ the password code written in the memory of a portable telephone 1 ] that automatic elimination is made to be carried out.

[0018] The management equipment 3 which received the password code checks a response with the cellular-phone number of the portable telephone 1 added and transmitted to a password code and this password code based on the file according to individual memorized by storage 31 from a portable telephone 1. Consequently, if a password code is right, management equipment 3 memorizes that there was an application of credit payment from a shopper, will turn the completion signal of reception to a portable telephone 1, and will transmit it. In addition, the application of credit payment will be canceled, if predetermined time amount (for example, for 1 - 30 minutes) passes after memorizing that there was the application. In this case, time with the application of credit payment, the time by which the application was canceled are recorded as hysteresis.

[0019] The reception code showing the data showing whether credit payment is permitted, the data showing the amount of money in which credit payment is possible, and a purport with the application of credit payment etc. is contained in the completion signal of reception sent to a portable telephone 1 from management equipment 3. The portable telephone 1 which received the completion signal of reception displays on a display 12 the content of the various data contained in the completion signal of reception. Therefore, a shopper can check whether credit payment is possible before payment of a goods price by seeing the display of a display 12.

[0020] the shopper (or salesclerk requested from the shopper) who checked that credit payment was possible -- next, a portable telephone 1 is connected to the store terminal 2. It sets to the exclusive holder 21 connected to the store terminal 2, and the connection between this portable telephone 1 and the store terminal 2 is attained by connecting

the holder side connection terminal prepared in this exclusive holder 21, and the telephone side connection terminal prepared in the portable telephone 1.

[0021] Connection of a portable telephone 1 and the store terminal 2 carries out reading appearance of the cellular-phone number of a portable telephone 1 to the store terminal 2 from the memory built in the portable telephone 1. And this cellular-phone number by which reading appearance was carried out is transmitted to management equipment 3 through a communication line from the store terminal 2. It checks whether management equipment 3 has had the application of credit payment from the portable telephone 1 corresponding to the cellular-phone number received from the store terminal 2. And when there is an application of credit payment in advance of reception of a cellular-phone number, the shopper (or shopper who requested connection of a portable telephone 1 from the salesclerk) who connected the portable telephone 1 to the store terminal 2 attests with his being the owner of a portable telephone 1, and transmits the signal of a purport with which credit payment is permitted (authentication O.K.) to the store terminal 2. On the other hand, when there is no application of credit payment in advance of reception of a cellular-phone number, the signal of a purport with which credit payment is not permitted is transmitted to the store terminal 2.

[0022] If the signal of a purport with which credit payment is permitted is received by the store terminal 2, the salesclerk who the purport which may receive credit payment was displayed on the display 22 of the store terminal 2, and looked at this display permits payment of the goods price by credit payment to a shopper. And if a salesclerk inputs the amount of a goods price etc. into the store terminal 2, the data of the amount of the inputted goods price will be sent to management equipment 3, and the amount-of-money data will be written in the file according to individual of the shopper using credit payment (storage 31) by management equipment 3. The amount-of-money data written in the file according to individual are totaled by that day or later, and the amount of money according to the totaled amount-of-money data is pulled down from the shopper's bank account on the delivery date set beforehand.

[0023] In not checking a password code according to this operation gestalt as mentioned above when management equipment 3 receives a cellular-phone number from the store terminal 2 since a password code is transmitted to management equipment 3 from a portable telephone 1 and it is checked for the password code in advance of payment of the goods price by credit payment at this time whether it is the right, it is not necessary to call a portable telephone 1 from management equipment 3. Therefore, as compared with the conventional technique (for example, system currently indicated by JP,11-45366,A), the time amount taken [ after connecting a portable telephone 1 to the store terminal 2 ] to complete personal authentication (until credit payment is permitted) can be shortened.

[0024] Moreover, according to this operation gestalt, the shopper who the completion signal of reception is sent to a portable telephone 1 from management equipment 3, and is going to use credit payment for it since the information about credit payment which said if you please whether credit payment would be possible is displayed on the display 12 of a portable telephone 1 can check whether credit payment is possible before payment of a goods price by seeing the display of a display 12.

[0025] Drawing 2 is the block diagram showing the whole personal authentication system configuration concerning other operation gestalten of this invention. The personal authentication system which the personal authentication system concerning this operation gestalt requires for the operation gestalt of drawing 1 mentioned above, and the hard configuration are almost the same, and configurations like software, such as communication link sequence between a portable telephone 1, the store terminal 2, and management equipment 3, differ. Therefore, at drawing 2, the same reference mark as the case of drawing 1 is attached and shown in the part equivalent to each part shown in above-mentioned drawing 1, and, below, explanation of the hard configuration of the personal authentication system concerning this operation gestalt is omitted.

[0026] For example in advance of payment of the goods price by that credit payment, the shopper who is going to pay a goods price by credit payment operates the input key 11 of his own portable telephone 1, inputs a password code, and makes the memory in which that inputted password code was contained by the portable telephone 1 memorize with this operation gestalt. In order to prevent that reading appearance of the password code is carried out, and the password code memorized by this memory is used improperly from the memory of a portable telephone 1 when the case where the theft of the portable telephone 1 is carried out, and a portable telephone 1 are lost, After predetermined time (for example, for 2 minutes) passes since the writing, as for the password code written in the memory of a portable telephone 1, it is desirable that automatic elimination is made to be carried out.

[0027] a shopper (or salesclerk requested from the shopper) -- next, a portable telephone 1 is connected to the store terminal 2. Connection of a portable telephone 1 and the store terminal 2 carries out reading appearance of the cellular-phone number of a portable telephone 1 to the store terminal 2 from the memory built in the portable telephone 1. And this cellular-phone number by which reading appearance was carried out is transmitted to management equipment 3 through a communication line from the store terminal 2. The management equipment 3 which received the cellular-phone number from the store terminal 2 calls the portable telephone 1 of the received cellular-phone number. If the shopper who has noticed the call of a portable telephone 1 answers a call, reading appearance of the password code memorized by the memory built in the portable telephone 1 will be carried out automatically, and the password code by which reading appearance was carried out will be automatically transmitted towards management equipment 3 (if the call carbon button of a portable telephone 1 is pushed).

[0028] Management equipment 3 will check a response with this received password code and the cellular-phone number received from the store terminal 2 based on the file according to individual memorized by storage 31, if a password code is received from a portable telephone 1. Consequently, if a password code is right, the shopper (or shopper who requested connection of a portable telephone 1 from the salesclerk) who connected the portable telephone 1 to the store terminal 2 attests with his being the owner of a portable telephone 1, the signal of a purport with which credit payment is permitted to the store terminal 2 from management equipment 3 (authentication O.K.) is transmitted, and if a password code is not right, the signal of a purport with which credit payment is not permitted will be transmitted to a store terminal 2 from management equipment 3.

[0029] If the signal of a purport with which credit payment is permitted is received by the store terminal 2, the salesclerk who the purport which may receive credit payment was displayed on the display 22 of the store terminal 2, and looked at this display permits payment of the goods price by credit payment to a shopper. And if a salesclerk inputs the amount of a goods price etc. into the store terminal 2, the data of the amount of the inputted goods price will be sent to management equipment 3, and the amount-of-money data will be written in the file according to individual of the shopper using credit payment (storage 31) by management equipment 3. The amount-of-money data written in the file according to individual are totaled by that day or later, and the amount of money according to the totaled amount-of-money data is pulled down from the shopper's bank account on the delivery date set beforehand.

[0030] If according to this operation gestalt the password code is beforehand stored in the memory built in the portable telephone 1 and the call of the portable telephone 1 from management equipment 3 is answered, the password code stored in that memory will be automatically transmitted towards management equipment 3. Thereby, after there is a call of a portable telephone 1 from management equipment 3, the input key 11 of a portable telephone 1 can be operated, a password code can be inputted, and the time amount which personal authentication takes can be shortened compared with the conventional technique which turns this inputted password code to management equipment 3, and is transmitted.

[0031] As mentioned above, although two operation gestalten of this invention were explained, this invention can also be carried out with the gestalt of further others. For example, although [ each above-mentioned operation gestalt ] the cellular-phone number is memorized by the memory built in the portable telephone 1 and reading appearance of this cellular-phone number is carried out to the store terminal 2, the memory of a portable telephone 1 stores the ID code of a proper etc. in a portable telephone 1, this ID code is read to the store terminal 2, and you may make it transmit to management equipment 3. In this case, the ID code of a proper will be further written in a portable telephone 1 at the file according to individual memorized by the storage 31 of management equipment 3.

[0032] Moreover, the memory of a portable telephone 1 is made to memorize the reception code contained in the completion signal of reception transmitted to a portable telephone 1 from management equipment 3 in the case of the 1st above-mentioned operation gestalt, this reception code is read to the store terminal 2, and you may make it transmit to management equipment 3. In this case, in case a reception code (the completion signal of reception) is transmitted towards a portable telephone 1 from management equipment 3, it is desirable to write this reception code in the file according to individual in the storage 31 of management equipment 3.

[0033] Furthermore, although [ each above-mentioned operation gestalt ] cable connection of a portable telephone 1 and the store terminal 2 is made by setting a portable telephone 1 to the exclusive holder 21, a portable telephone 1 and the store terminal 2 may be equipped with a wireless data communications interface respectively like Bluetooth, and the data transmission and reception between a portable telephone 1 and the store terminal 2 may be attained by radiocommunication, for example. furthermore -- a \*\*\*\* -- operation -- a gestalt -- \*\*\*\* -- personal authentication -- a system -- a credit -- payment -- depending -- goods -- a price -- payment -- the time -- using -- having -- a case -- an example -- taking -- having explained -- although -- this -- invention -- starting -- personal authentication -- a system -- a bank -- etc. -- installing -- having had -- a cash dispenser -- ( -- CD -- ) -- a machine -- cash -- pulling out -- the time -- it can set -- personal authentication -- a sake -- using -- you may have .

[0034] In addition, it is possible to perform design changes various in the range of the matter indicated by the claim.

---

[Translation done.]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-7698

(P2002-7698A)

(43)公開日 平成14年1月11日(2002.1.11)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テマート*(参考)
G 0 6 F 17/60	2 2 2	G 0 6 F 17/60	2 2 2 5 B 0 4 9
	4 1 4		4 1 4 5 B 0 5 5
	5 0 6		5 0 6 5 B 0 8 5
15/00	3 3 0	15/00	3 3 0 G 5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 A
審査請求 未請求 請求項の数6 O L (全 8 頁)			

(21)出願番号 特願2000-183325(P2000-183325)

(22)出願日 平成12年6月19日(2000.6.19)

(71)出願人 000169477

高砂電器産業株式会社

大阪府大阪市中央区南船場2丁目9番14号

(72)発明者 西村 孝之

大阪府大阪市中央区南船場2丁目9番14号

高砂電器産業株式会社内

(74)代理人 100087701

弁理士 稲岡 耕作 (外2名)

Fターム(参考) 5B049 AA06 CC36 EE08 GG03 GG06  
GG10

5B055 HA04 HA12

5B085 AE04 AE23

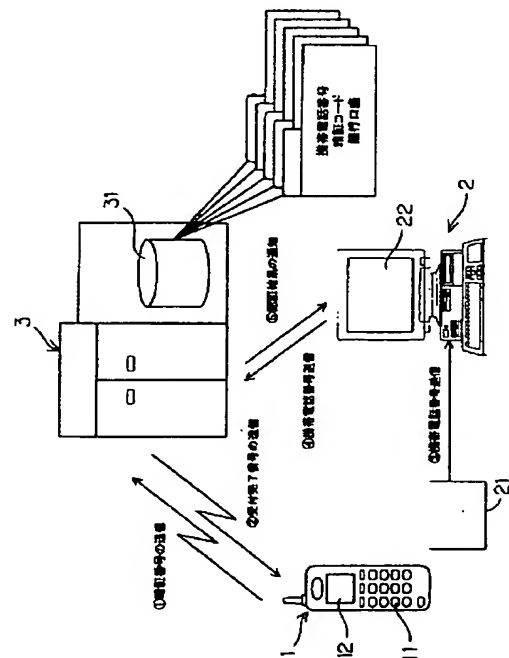
5J104 AA07 KA01 NA05 PA02 PA10

(54)【発明の名称】 個人認証システム、個人認証方法および管理装置

(57)【要約】

【課題】認証に要する時間を短縮できる個人認証システムおよび個人認証方法を提供する。

【解決手段】クレジット払いで商品代金を支払おうとする買い物客は、その商品代金の支払いに先立って、自分の携帯電話機1から管理装置3を呼び出し、暗証コードを入力して管理装置3に送信する。正しい暗証コードを送信すると、管理装置3から携帯電話機1に受付完了信号が送られてくる。その後、買い物客によって携帯電話機1が店舗端末機2に接続されると、携帯電話機1に内蔵されているメモリから携帯電話番号が店舗端末機2に読み出され、その携帯電話番号が店舗端末機2から管理装置3に送信される。管理装置3は、店舗端末機2から受信した携帯電話番号に対応する携帯電話機1からクレジット払いの申込みがあったかどうかを確認し、申込みがあった場合には、クレジット払いを許可する旨の信号を店舗端末機2に送信する。



## 【特許請求の範囲】

【請求項1】 認証を受けようとする場所に備えられ、個人が所有する携帯通信機から当該携帯通信機の識別情報を検出することのできる端末機と、この端末機と通信回線を介して接続され、個人を認証するために必要な携帯通信機の識別情報および暗証コードが関連づけて記憶された記憶手段を備えた管理装置とを含む個人認証システムであって、

上記端末機は、携帯通信機の識別情報を検出して、この検出した識別情報を上記管理装置に向けて送信するものであり、

上記管理装置は、携帯通信機から識別情報および暗証コードを受信したときに、この受信した暗証コードが当該携帯通信機の識別情報に関連づけて上記記憶手段に記憶されている暗証コードと一致するか否かを確認して、一致したときに当該携帯通信機を所有している個人から認証の申込みがあったことを記憶しておき、その後上記端末機から識別情報を受信したときに、この受信した識別情報により特定される携帯通信機から以前に認証の申込みがあったかどうかを確認して、認証の申込みがあったことが確認された場合には、上記端末機に向けて認証OKの返事を送信するものであることを特徴とする個人認証システム。

【請求項2】 上記管理装置は、携帯通信機から受信した暗証コードが当該携帯通信機の識別情報に関連づけて上記記憶手段に記憶されている暗証コードと一致し、当該携帯通信機を所有している個人から認証の申込みがあったことを記憶した場合に、暗証コード受付完了信号を当該携帯通信機に送信する手段を含むことを特徴とする請求項1記載の個人認証システム。

【請求項3】 認証を受けようとする場所に備えられ、個人が所有する携帯通信機から当該携帯通信機の識別情報を検出することのできる端末機と、この端末機と通信回線を介して接続され、個人を認証するために必要な携帯通信機の識別情報および暗証コードが関連づけて記憶された記憶手段を備えた管理装置とを含む個人認証システムであって、

上記端末機は、携帯通信機の識別情報を検出して、この検出した識別情報を上記管理装置に向けて送信するものであり、

上記管理装置は、上記端末機から携帯通信機の識別情報を受信すると、この識別情報により特定される携帯通信機を呼び出し、その後、この呼出しに回答して携帯通信機から自動的に送信されてくる暗証コードを受信したときに、この受信した暗証コードが当該携帯通信機の識別情報に関連づけて上記記憶手段に記憶されている暗証コードと一致するか否かを確認して、一致することを確認した場合には、上記端末機に向けて認証OKの返事を送信するものであることを特徴とする個人認証システム。

【請求項4】 個人が所有する携帯通信機を利用して、そ

の個人を認証する方法であって、

携帯通信機によって、管理装置に対して当該携帯通信機の識別情報および暗証コードを予め送信しておき、

認証を受けようとする場所に備えられた端末機に携帯通信機の識別情報を検出させ、

この携帯通信機の識別情報を検出した端末機は、その検出した識別情報を通信回線を介して上記管理装置に送り、

上記管理装置は、携帯通信機から識別情報および暗証コードを受信したときに、この受信した暗証コードが当該携帯通信機の識別情報に関連づけて記憶手段に記憶されている暗証コードと一致するか否かを確認して、一致したときに当該携帯通信機を所有している個人から認証の申込みがあったことを記憶しておき、その後上記端末機から識別情報を受信したときに、この受信した識別情報により特定される携帯通信機から以前に認証の申込みがあったかどうかを確認して、認証の申込みがあったことが確認された場合には、上記端末機に向けて認証OKの返事を送信することを特徴とする個人認証方法。

【請求項5】 個人が所有する携帯通信機を利用して、その個人を認証する方法であって、

携帯通信機に暗証コードを予め入力して記憶させておき、

認証を受けようとする場所に備えられた端末機に携帯通信機の識別情報を検出させ、

この携帯通信機の識別情報を検出した端末機は、その検出した識別情報を通信回線を介して管理装置に送り、

管理装置は、上記端末機から携帯通信機の識別情報を受信すると、この識別情報により特定される携帯通信機を呼び出し、

この呼出しを受けた携帯通信機は、予め入力されて記憶している暗証コードを自動的に管理装置に向けて送信し、

携帯通信機から暗証コードを受信した管理装置は、この受信した暗証コードが当該携帯通信機の識別情報に関連づけて記憶手段に記憶されている暗証コードと一致するか否かを確認して、一致することを確認した場合には、上記端末機に向けて認証OKの返事を送信することを特徴とする個人認証方法。

【請求項6】 個人が所有する携帯通信機を利用して、その個人を認証する個人認証システム用の管理装置であって、

個人を認証するために必要な携帯通信機の識別情報および暗証コードが関連づけて記憶された記憶手段を備えていて、

認証を受けようとする場所に設置された端末機が接続されているとともに、携帯通信機と通信可能であり、

携帯通信機から識別情報および暗証コードを受信したときに、この受信した暗証コードが当該携帯通信機の識別情報に関連づけて上記記憶手段に記憶されている暗証コ

ードと一致するか否かを確認して、一致したときに当該携帯通信機を所有している個人から認証の申込みがあったことを記憶しておき、その後に上記端末機から識別情報を受信したときに、この受信した識別情報により特定される携帯通信機から以前に認証の申込みがあったかどうかを確認して、認証の申込みがあったことが確認された場合には、上記端末機に向けて認証OKの返事を送信するものであることを特徴とする管理装置。

#### 【発明の詳細な説明】

##### 【0001】

【発明の属する技術分野】この発明は、携帯通信機を用いて個人の認証を行う個人認証システム、個人認証方法および個人認証システム用の管理装置に関する。

##### 【0002】

【従来の技術】たとえば、商品代金をクレジットカードで支払う際や、銀行などに設置されたキャッシュディスプレイ（ＣＤ）機で現金を引き出す際には、クレジットカードまたはキャッシュディスプレイ機の利用者の認証（個人認証）が行われる。この個人認証は、クレジットカードまたはキャッシュカードに記録されている情報などに基づいて行われるのが一般的であるが、最近では、たとえば特開平11-45366号公報に開示されているシステムなど、携帯電話機を用いて個人認証を行う手法が提案されている。

【0003】上記公開公報に開示されているシステムでは、買い物客は、店舗で購入した商品の代金を支払う際に、自分の携帯電話機を店舗に設置されている端末機に接続する。携帯電話機と端末機とが接続されると、携帯電話機の呼出し番号（携帯電話番号）が端末機に読み出され、その読み出された呼出し番号が、システムを統括管理しているコンピュータに送信される。その後、コンピュータに送られてきた呼出し番号に基づき、コンピュータから買い物客の携帯電話機が呼び出される。この呼出しに買い物客が応答すると、コンピュータから暗証コードを入力するように案内され、この案内に従って買い物客が暗証コードを携帯電話機に入力すると、その暗証コードがコンピュータに送信される。コンピュータには、予め携帯電話機の呼出し番号とその所有者に付与された暗証コードとが関連づけられて登録されており、携帯電話機から暗証コードが送られてくると、この送られてきた暗証コードと登録されている暗証コードとが照合が行われ、これらの暗証コードが一致すれば、その携帯電話機に暗証コードを入力した者は携帯電話機の所有者であると認証される。こうして認証がなされると、後日、携帯電話機の所有者の銀行口座から商品代金が引き落とされる。

##### 【0004】

【発明が解決しようとする課題】上述のように、上記公開公報に開示されているシステムでは、携帯電話機を端末機に接続した後、コンピュータから携帯電話機が呼び

出されるまで待ち、携帯電話機が呼び出されたことに応答して暗証コードを入力すると、その入力した暗証コードがコンピュータに送信されて認証が行われる。そのため、携帯電話機を端末機に接続してから認証が完了するまでに長い時間かかり、買い物客を苛立たせるかもしれない。また、とくに店が混雑しているときに認証に時間がかかると、他の買い物客を待たせることになり、これらの他の買い物客や店員まで苛々させるかもしれない。

【0005】そこで、この発明の目的は、上述の技術的課題を解決し、認証に要する時間を短縮できる個人認証システム、個人認証方法および個人認証システム用の管理装置を提供することである。

##### 【0006】

【課題を解決するための手段および発明の効果】上記の目的を達成するための請求項1記載の発明は、認証を受けようとする場所に備えられ、個人が所有する携帯通信機から当該携帯通信機の識別情報を検出することのできる端末機と、この端末機と通信回線を介して接続され、個人を認証するために必要な携帯通信機の識別情報および暗証コードが関連づけて記憶された記憶手段を備えた管理装置とを含む個人認証システムであって、上記端末機は、携帯通信機の識別情報を検出して、この検出した識別情報を上記管理装置に向けて送信するものであり、上記管理装置は、携帯通信機から識別情報および暗証コードを受信したときに、この受信した暗証コードが当該携帯通信機の識別情報に関連づけて上記記憶手段に記憶されている暗証コードと一致するか否かを確認して、一致したときに当該携帯通信機を所有している個人から認証の申込みがあったことを記憶しておき、その後に上記端末機から識別情報を受信したときに、この受信した識別情報により特定される携帯通信機から以前に認証の申込みがあったかどうかを確認して、認証の申込みがあったことが確認された場合には、上記端末機に向けて認証OKの返事を送信するものであることを特徴とする個人認証システムである。

【0007】この発明によれば、携帯通信機から管理装置に暗証コードが送信され、このとき暗証コードが正しいか否かが確認されているから、管理装置が端末機から携帯通信機の識別情報を受信したときに、この識別情報と暗証コードとの対応関係の確認を行う必要がない。ゆえに、管理装置が端末機から受信した携帯通信機の識別情報（携帯電話番号など）により識別される携帯通信機を呼び出し、この呼出しがあった後に暗証コードを入力して管理装置に送信する従来技術に比べ、通信機識別情報受信手段が通信機識別情報を受信してから個人認証が完了するまでに要する時間を短縮することができる。

【0008】なお、請求項2に記載のように、上記管理装置は、携帯通信機から受信した暗証コードが当該携帯通信機の識別情報に関連づけて上記記憶手段に記憶されている暗証コードと一致し、当該携帯通信機を所有して

いる個人から認証の申込みがあったことを記憶した場合に、暗証コード受付完了信号を当該携帯通信機に送信する手段を含むことが好ましい。この場合、暗証コード受付完了信号が携帯通信機に送信されるから、暗証コードを携帯通信機から管理装置に送信した個人は、送信した暗証コードが正しいものであったか否かを知ることができる。

【0009】請求項3記載の発明は、認証を受けようとする場所に備えられ、個人が所有する携帯通信機から当該携帯通信機の識別情報を検出することのできる端末機と、この端末機と通信回線を介して接続され、個人を認証するために必要な携帯通信機の識別情報および暗証コードが関連づけて記憶された記憶手段を備えた管理装置とを含む個人認証システムであって、上記端末機は、携帯通信機の識別情報を検出して、この検出した識別情報を上記管理装置に向けて送信するものであり、上記管理装置は、上記端末機から携帯通信機の識別情報を受信すると、この識別情報により特定される携帯通信機を呼び出し、その後、この呼出しに応答して携帯通信機から自動的に送信されてくる暗証コードを受信したときに、この受信した暗証コードが当該携帯通信機の識別情報に関連づけて上記記憶手段に記憶されている暗証コードと一致するか否かを確認して、一致することを確認した場合には、上記端末機に向けて認証OKの返事を送信するものであることを特徴とする個人認証システムである。

【0010】この発明によれば、管理装置への通信機識別情報の送信に先立って携帯通信機に暗証コードが入力されており、管理装置からの携帯通信機の呼出しに应答すると、その先立って入力されている暗証コードが管理装置に向けて自動送信される。これにより、管理装置から携帯通信機の呼出しがあった後に、携帯通信機に暗証コードを入力し、この入力した暗証コードを管理装置に向けて送信する従来技術と比べ、個人認証に要する時間を短縮することができる。

【0011】請求項4記載の発明は、個人が所有する携帯通信機を利用して、その個人を認証する方法であって、携帯通信機によって、管理装置に対して当該携帯通信機の識別情報および暗証コードを予め送信しておき、認証を受けようとする場所に備えられた端末機に携帯通信機の識別情報を検出させ、この携帯通信機の識別情報を検出した端末機は、その検出した識別情報を通信回線を介して上記管理装置に送り、上記管理装置は、携帯通信機から識別情報および暗証コードを受信したときに、この受信した暗証コードが当該携帯通信機の識別情報に関連づけて記憶手段に記憶されている暗証コードと一致するか否かを確認して、一致したときに当該携帯通信機を所有している個人から認証の申込みがあったことを記憶しておき、その後に上記端末機から識別情報を受信したときに、この受信した識別情報により特定される携帯通信機から以前に認証の申込みがあったかどうかを確認

して、認証の申込みがあったことが確認された場合には、上記端末機に向けて認証OKの返事を送信することを中心とする個人認証方法である。

【0012】この方法によれば、請求項1に関連して述べた効果と同様の効果を得ることができる。請求項5記載の発明は、個人が所有する携帯通信機を利用して、その個人を認証する方法であって、携帯通信機に暗証コードを予め入力して記憶させておき、認証を受けようとする場所に備えられた端末機に携帯通信機の識別情報を検出させ、この携帯通信機の識別情報を検出した端末機は、その検出した識別情報を通信回線を介して管理装置に送り、管理装置は、上記端末機から携帯通信機の識別情報を受信すると、この識別情報により特定される携帯通信機を呼び出し、この呼出しを受けた携帯通信機は、予め入力されて記憶している暗証コードを自動的に管理装置に向けて送信し、携帯通信機から暗証コードを受信した管理装置は、この受信した暗証コードが当該携帯通信機の識別情報に関連づけて記憶手段に記憶されている暗証コードと一致するか否かを確認して、一致することを確認した場合には、上記端末機に向けて認証OKの返事を送信することを中心とする個人認証方法である。

【0013】この方法によれば、請求項3に関連して述べた効果と同様の効果を得ることができる。請求項6記載の発明は、個人が所有する携帯通信機を利用して、その個人を認証する個人認証システム用の管理装置であって、個人を認証するために必要な携帯通信機の識別情報および暗証コードが関連づけて記憶された記憶手段を備えていて、認証を受けようとする場所に設置された端末機が接続されているとともに、携帯通信機と通信可能であり、携帯通信機から識別情報および暗証コードを受信したときに、この受信した暗証コードが当該携帯通信機の識別情報に関連づけて上記記憶手段に記憶されている暗証コードと一致するか否かを確認して、一致したときに当該携帯通信機を所有している個人から認証の申込みがあったことを記憶しておき、その後に上記端末機から識別情報を受信したときに、この受信した識別情報により特定される携帯通信機から以前に認証の申込みがあったかどうかを確認して、認証の申込みがあったことが確認された場合には、上記端末機に向けて認証OKの返事を送信するものであることを特徴とする管理装置である。

【0014】この発明の管理装置を用いた個人認証システムでは、請求項1に関連して述べた効果と同様な効果を得ることができる。

【0015】

【発明の実施の形態】以下では、この発明の実施の形態を、添付図面を参照して詳細に説明する。図1は、この発明の一実施形態に係る個人認証システムの全体構成を示すブロック図である。この個人認証システムは、たとえば、街中の店舗などで買い物をした買い物客が商品代

金をクレジット払い（店舗で現金を支払わずに、後日に商品代金が銀行口座から引き落とされることにより商品代金を支払う方法）で支払うときに利用されるシステムであり、各買い物客の所有する携帯電話機1を用いる。携帯電話機1には、図示しないメモリが内蔵されており、このメモリには、携帯電話機1を呼び出すための呼出し番号（携帯電話番号）や所有者が入力キー11を操作して入力した番号などを記憶させておくことができるようになっている。

【0016】各店舗には、個人認証を行うための店舗端末機2が設置されている。店舗端末機2は、通信回線を介して、この個人認証システムを統括管理するクレジット会社や銀行など（以下、「システム運用会社」という。）に設置された管理装置3に接続されている。また、管理装置3は、たとえば電話回線網を介して、携帯電話機1との間でデータ通信を行うことができるようになっている。管理装置3には、個人別ファイルを記憶するための記憶装置31が備えられている。個人別ファイルは、たとえば、個人がシステム運用会社と個人認証システムの利用契約を結んだときに作成されて記憶装置31に記憶されるものであり、個人（買い物客）の携帯電話機1の携帯電話番号、個人に付与された暗証コード、商品代金を引き落とすための個人の銀行口座などの情報を含む。暗証コードは、たとえば、個人認証システムの利用契約の際に個人が決定することができ、複数の数字や文字の組み合わせで構成される。すなわち、管理装置3の記憶装置31には、個人認証に必要な携帯電話番号、暗証コードおよび銀行口座などの情報が互に関連づけられて個人別に記憶されている。

【0017】たとえば、クレジット払いで商品代金を支払おうとする買い物客は、その商品代金の支払いに先立って、自分の携帯電話機1から管理装置3を呼び出し、携帯電話機1の入力キー11を操作して暗証コードを管理装置3に送信する。管理装置3の呼出し番号は、携帯電話機1のメモリに予め記憶させておいてもよいし、管理装置3を呼び出す度に入力キー11を操作して入力してもよい。また、暗証コードも、携帯電話機1に内蔵されたメモリに予め記憶させておいてもよいし、管理装置3を呼び出す度に入力キー11を操作して入力してもよい。ただし、携帯電話機1が盗難された場合や携帯電話機1を紛失した場合などに、携帯電話機1のメモリから暗証コードが読み出されて不正使用されることを防止するため、携帯電話機1のメモリに書き込まれた暗証コードは、その書き込みから所定時間（たとえば、2分間）が経過した後に自動消去されるようにしておくことが好ましい。

【0018】携帯電話機1から暗証コードを受信した管理装置3は、たとえば、暗証コードとこの暗証コードに付加されて送信されてくる携帯電話機1の携帯電話番号との対応を記憶装置31に記憶されている個人別ファイ

ルに基づいて確認する。その結果、暗証コードが正しければ、管理装置3は、買い物客からクレジット払いの申込みがあったことを記憶し、受付完了信号を携帯電話機1に向けて送信する。なお、クレジット払いの申込みは、その申込みがあったことを記憶してから所定の時間（たとえば、1〜30分間）が経過するとキャンセルされる。この場合、クレジット払いの申込みのあった日時や申込みがキャンセルされた日時などが履歴として記録される。

【0019】管理装置3から携帯電話機1に送られてくる受付完了信号には、クレジット払いを許可するか否かを表すデータ、クレジット払いが可能な金額を表すデータ、クレジット払いの申込みがあった旨を表す受付コードなどが含まれている。受付完了信号を受信した携帯電話機1は、受付完了信号に含まれている種々のデータの内容をディスプレイ12に表示させる。したがって、買い物客は、ディスプレイ12の表示を見ることにより、クレジット払いが可能であるかどうかなどを商品代金の支払い前に確認することができる。

【0020】クレジット払いが可能であることを確認した買い物客（または買い物客に依頼された店員）は、次に、携帯電話機1を店舗端末機2に接続する。この携帯電話機1と店舗端末機2との接続は、たとえば、店舗端末機2に接続された専用ホルダ21にセットし、この専用ホルダ21に設けられているホルダ側接続端子と携帯電話機1に設けられている電話機側接続端子とを接続することにより達成される。

【0021】携帯電話機1と店舗端末機2とが接続されると、携帯電話機1に内蔵されているメモリから、携帯電話機1の携帯電話番号が店舗端末機2に読み出される。そして、この読み出された携帯電話番号が、店舗端末機2から通信回線を介して管理装置3に送信される。管理装置3は、店舗端末機2から受信した携帯電話番号に対応する携帯電話機1からクレジット払いの申込みがあったかどうかを確認する。そして、携帯電話番号の受信に先立ってクレジット払いの申込みがあった場合には、店舗端末機2に携帯電話機1を接続した買い物客（または店員に携帯電話機1の接続を依頼した買い物客）は携帯電話機1の所有者であると認証して、クレジット払いを許可（認証OK）する旨の信号を店舗端末機2に送信する。一方、携帯電話番号の受信に先立ってクレジット払いの申込みがない場合には、クレジット払いを許可しない旨の信号を店舗端末機2に送信する。

【0022】クレジット払いを許可する旨の信号が店舗端末機2に受信されると、店舗端末機2のディスプレイ22にクレジット払いを受け付けてもよい旨が表示され、この表示を見た店員は、買い物客に対してクレジット払いによる商品代金の支払いを許可する。そして、店員が商品代金の金額などを店舗端末機2に入力すると、その入力された商品代金の金額のデータが管理装置3に

送られ、管理装置3によって、その金額データがクレジット払いを利用した買い物客の個人別ファイル（記憶装置31）に書き込まれる。個人別ファイルに書き込まれた金額データは、当日または後日に集計され、その集計された金額データに応じた金額が、その買い物客の銀行口座から予め定める決済日に引き落とされる。

【0023】以上のようにこの実施形態によれば、クレジット払いによる商品代金の支払いに先立って、携帯電話機1から管理装置3に暗証コードが送信され、このとき暗証コードが正しいか否かが確認されているから、管理装置3が店舗端末機2から携帯電話番号を受信したときに暗証コードの確認を行う必要がないうえ、管理装置3から携帯電話機1を呼び出す必要もない。ゆえに、従来技術（たとえば、特開平11-45366号公報に開示されているシステム）と比較して、携帯電話機1を店舗端末機2に接続してから個人認証が完了するまで（クレジット払いが許可されるまで）に要する時間を短縮できる。

【0024】また、この実施形態によれば、管理装置3から携帯電話機1に受付完了信号が送られて、携帯電話機1のディスプレイ12に、クレジット払いが可能であるかどうかといったようなクレジット払いに関する情報が表示されるから、クレジット払いを利用しようとする買い物客は、ディスプレイ12の表示を見ることにより、クレジット払いが可能であるかどうかなどを商品代金の支払い前に確認することができる。

【0025】図2は、この発明の他の実施形態に係る個人認証システムの全体構成を示すブロック図である。この実施形態に係る個人認証システムは、上述した図1の実施形態に係る個人認証システムとハード的な構成はほぼ同様であり、携帯電話機1、店舗端末機2および管理装置3間における通信順序などのソフト的な構成が異なる。したがって、図2では、上述の図1に示す各部に相当する部分に、図1の場合と同一の参照符号を付して示し、以下では、この実施形態に係る個人認証システムのハード構成の説明を省略する。

【0026】この実施形態では、クレジット払いで商品代金を支払おうとする買い物客は、たとえば、そのクレジット払いによる商品代金の支払いに先立って、自分の携帯電話機1の入力キー11を操作して暗証コードを入力して、その入力した暗証コードを携帯電話機1に内蔵されたメモリに記憶させておく。このメモリに記憶された暗証コードは、携帯電話機1が盗難された場合や携帯電話機1を紛失した場合などに、携帯電話機1のメモリから暗証コードが読み出されて不正使用されることを防止するため、携帯電話機1のメモリに書き込まれた暗証コードは、その書き込みから所定時間（たとえば、2分間）が経過した後に自動消去されるようにしておくことが好ましい。

【0027】買い物客（または買い物客に依頼された店

員）は、次に、携帯電話機1を店舗端末機2に接続する。携帯電話機1と店舗端末機2とが接続されると、携帯電話機1に内蔵されているメモリから、携帯電話機1の携帯電話番号が店舗端末機2に読み出される。そして、この読み出された携帯電話番号が、店舗端末機2から通信回線を介して管理装置3に送信される。店舗端末機2から携帯電話番号を受信した管理装置3は、その受信した携帯電話番号の携帯電話機1を呼び出す。携帯電話機1の呼び出しに気づいた買い物客が呼び出しに应答すると（携帯電話機1の通話ボタンを押すと）、携帯電話機1に内蔵されたメモリに記憶されている暗証コードが自動的に読み出され、その読み出された暗証コードが管理装置3に向けて自動送信される。

【0028】管理装置3は、携帯電話機1から暗証コードを受信すると、この受信した暗証コードと店舗端末機2から受信した携帯電話番号との対応を記憶装置31に記憶されている個人別ファイルに基づいて確認する。その結果、暗証コードが正しければ、店舗端末機2に携帯電話機1を接続した買い物客（または店員に携帯電話機1の接続を依頼した買い物客）は携帯電話機1の所有者であると認証して、管理装置3から店舗端末機2にクレジット払いを許可（認証OK）する旨の信号が送信され、暗証コードが正しくなければ、管理装置3から店舗端末機2にクレジット払いを許可しない旨の信号が送信される。

【0029】クレジット払いを許可する旨の信号が店舗端末機2に受信されると、店舗端末機2のディスプレイ22にクレジット払いを受け付けてもよい旨が表示され、この表示を見た店員は、買い物客に対してクレジット払いによる商品代金の支払いを許可する。そして、店員が商品代金の金額などを店舗端末機2に入力すると、その入力された商品代金の金額のデータが管理装置3に送られ、管理装置3によって、その金額データがクレジット払いを利用した買い物客の個人別ファイル（記憶装置31）に書き込まれる。個人別ファイルに書き込まれた金額データは、当日または後日に集計され、その集計された金額データに応じた金額が、その買い物客の銀行口座から予め定める決済日に引き落とされる。

【0030】この実施形態によれば、携帯電話機1に内蔵されたメモリに暗証コードが予め格納されており、管理装置3からの携帯電話機1の呼出しに应答すると、そのメモリに格納された暗証コードが管理装置3に向けて自動送信される。これにより、管理装置3から携帯電話機1の呼出しがあった後に、携帯電話機1の入力キー11を操作して暗証コードを入力し、この入力した暗証コードを管理装置3に向けて送信する従来技術と比べ、個人認証に要する時間を短縮することができる。

【0031】以上、この発明の2つの実施形態について説明したが、この発明は、さらに他の形態で実施することもできる。たとえば、上述の各実施形態では、携帯電

10

20

30

40

50

話機1に内蔵されているメモリには携帯電話番号が記憶されていて、この携帯電話番号が店舗端末機2に読み出されるとしたが、携帯電話機1のメモリに携帯電話機1に固有のIDコードなどを記憶させておき、このIDコードを店舗端末機2に読み出して管理装置3に送信するようにしてもよい。この場合、管理装置3の記憶装置31に記憶されている個人別ファイルには、携帯電話機1に固有のIDコードがさらに書き込まれることになる。

【0032】また、上述の第1の実施形態の場合には、管理装置3から携帯電話機1に送信される受付完了信号に含まれる受付コードを携帯電話機1のメモリに記憶させて、この受付コードを店舗端末機2に読み出して管理装置3に送信するようにしてもよい。この場合、管理装置3から携帯電話機1に向けて受付コード（受付完了信号）を送信する際に、この受付コードを管理装置3の記憶装置31内の個人別ファイルに書き込むことが好ましい。

【0033】さらに、上述の各実施形態では、携帯電話機1を専用ホルダ21にセットすることにより、携帯電話機1と店舗端末機2とが有線接続されるとしたが、たとえば、携帯電話機1および店舗端末機2にそれぞれBluetoothのような無線データ通信用インタフェースが備えられ、携帯電話機1および店舗端末機2間のデータ送\*

\* 受が無線通信により達成されてもよい。さらには、上述の実施形態では、個人認証システムがクレジット払いによる商品代金の支払いの際に利用される場合を例にとって説明したが、この発明に係る個人認証システムは、銀行などに設置されたキャッシュディスペンサ（CD）機で現金を引き出す際における個人認証のために利用されてもよい。

【0034】その他、特許請求の範囲に記載された事項の範囲で種々の設計変更を施すことが可能である。

#### 【図面の簡単な説明】

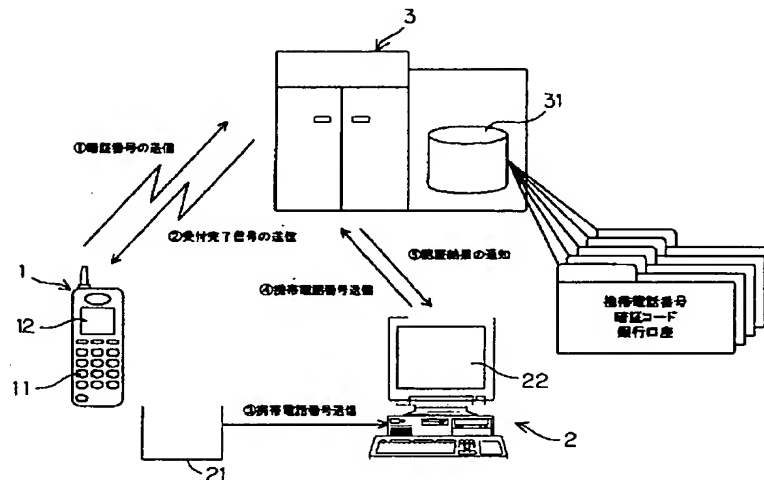
【図1】この発明の一実施形態に係る個人認証システムの全体構成を示すブロック図である。

【図2】この発明の他の実施形態に係る個人認証システムの全体構成を示すブロック図である。

#### 【符号の説明】

- |    |              |
|----|--------------|
| 1  | 携帯電話機（携帯通信機） |
| 2  | 店舗端末機（端末機）   |
| 3  | 管理装置         |
| 11 | 入力キー         |
| 12 | ディスプレイ       |
| 21 | 専用ホルダ        |
| 22 | ディスプレイ       |
| 31 | 記憶装置         |

【図1】



【図2】

